Topics:

network security [2], boundary [3], access [4]

Network Security - Boundary Protection [1]

SS-08-047 Network Security - Boundary Protection

Issue Date: 3/31/2008

Effective Date: 3/31/2008

PURPOSE

Controlling the flow of information into and out of the internal operational network and protecting it from malicious insiders, external entities with malicious intent, intentional or inadvertent denial of service attacks and unauthorized access or disclosure of sensitive information are essential activities of network security. Boundary or perimeter protection measures provide protection and monitoring capabilities against these and other threats to the network. Effective design, installation, configuration and maintenance of network boundary protection mechanisms are critical tasks in providing effective network security.

This standard establishes requirements for agencies to implement network boundary protection strategies.

STANDARD

Agencies shall establish controls that monitor and control the flow of information within and at the external boundary of the information systems and networks they operate.

Business Owners shall designate an individual (e.g. Agency ISO, CTO etc) responsible for managing and administering network boundary protection strategies (e.g. firewalls and other boundary protection devices).

Boundary Protection strategies shall include but are not limited to:

Physical Security: Agencies shall employ due diligence in ensuring physical security at any location where boundary protection devices are installed.

Access Control: All access to state information systems and networks shall be controlled and monitored in accordance with all enterprise access control policies and standards.

Interconnections: All connections to information systems outside the security boundary of an agency?s information system or the state backbone (internet, or other external network or information system) shall be fully documented, authorized, occur through controlled interfaces (e.g., proxies, gateways, routers, firewalls, encrypted tunnels) and be continuously monitored.

Least Functionality: Network boundary control devices shall be configured to provide only essential capabilities and specifically prohibit and/or restrict the use of functions, ports, protocols, and/or services. Agencies shall also monitor for inappropriate use of network services.

Default Denial: Agency firewalls shall block every network connectivity path and network service not explicitly authorized by the Agency ISO.

Configuration Changes and Documentation: All changes to firewall configuration parameters, enabled services, and